Jim Doyle, Governor

Rod Nilsestuen, Secretary

WISCONSIN

Office of Privacy Protection

Safeguarding Information for Your Future

Students and ID Theft: It Happens A Lot!
Tips for Online Protection

According to the Federal Trade Commission, persons aged 18-29 make up almost a third of all identity theft victims. Despite this fact, persons in this age group often are the last to find out that they have become id theft victims.

On average, an identity thief steals about $6,000 from each victim. Recovering from id theft costs the average victim nearly $1,500 in out-of-pocket expenses and takes countless hours of time. It is easier to protect yourself against identity theft than to recover from it and following are some tips for protection when you're online.

- **Know what you're downloading**
  It can be very tempting to download programs, games, screensavers, and the like, particularly if they are free. In fact, id thieves and others who want to mess with you try to make their download offers as enticing as possible so that you'll take advantage of their "great" offer. Know, however, that all downloading carries some risk. Viruses, spyware, and other software can come along with whatever it is you're downloading. Unless you feel really comfortable with wherever the download is coming from and exactly what the download contains, don't do it, particularly if it's free.

- **Beware of blogging**
  Blogging is very popular, but if you're not careful, it could result if your identity being stolen. To prevent this from happening to you, never post any personal identifying information other than your first name. This includes your date of birth, your address, and your phone number.

- **Make certain you have good security software and that you update it frequently**
  In order to be safe on line, you should have firewall, anti-virus, and anti-spyware software. Without this protection an identity thief can obtain such personal information such as your social security number and your bank account and credit numbers if you shop or pay bills on line. Since id thieves are always coming up with new ways to attack computers, you need to make certain that you update your anti-virus and anti-spyware software at least once per week. There is free software available if you can't afford to buy it yourself; for example, see Grisoft's free AVG anti-virus and Ewido anti-spyware software by visiting their website at http://free.grisoft.com.

- **Don't go phishing**
  Identity thieves get lots of help from us by simply asking for the information they want. They contact us by phone, email or regular mail posing as our bank, credit card company or even the IRS and ask us to "verify" information like account numbers, social security numbers or passwords. This is called "phishing" and id thieves are so good at it that they convince a lot of people that what is actually a fake website is the real thing. Legitimate companies or agencies don't ask for personal identifying information over the phone or on line, so if you're asked for it, it's likely to be an identity thief that's doing the asking. Never give out personal information unless you're the one who initiated the contact. When in doubt, find out the real phone number or web address through a different source and contact them to see if what you received was legitimate.

- **Protect your computer**
  Don't leave your computer unattended in your dorm room, the library or coffee house even if you're gone for only a minute. That minute might be all it takes to find information on your computer that will enable an id thief to steal your identity even if s/he doesn't steal your computer. Even if the computer, itself, is locked to something, lockdown your programs whenever you are away from your computer. You should turn on the feature that allows you to do this. It will take an extra 10 seconds to type in your password when you return, but it's time well spent.

- **Use passwords that are not easy to guess**
  Make certain your passwords aren't easy to guess. Names, addresses, birthdates, and even names of pets and friends can easily be figured out by those who know you even casually. If you want to be safe from identity theft, use passwords that are longer and will make no sense to anyone but you. Never use personally identifying information such as social security number, student id number or phone number as your password. In addition, change your passwords occasionally as an extra precaution.

- **Be careful about responding to online requests**
  Many sites on the internet ask for seemingly innocent information, such as what is your birthday, your favorite girl's name or the name of your dog. Such requests are particularly common in chat rooms, chain letters, blogs, and surveys. While the request may appear to be harmless, id thieves use the answers to try and figure out what your passwords might be. Don't give this information unless you're certain that you know who is asking for it and why.

- **Don't allow anyone else to share your computer or use your internet access**
  Identity thieves can install software on your computer that permits them to log every keystroke you make. If you permit someone else to use your computer or internet access, particularly if they use your computer more than one time, you run the risk of becoming an id theft victim. If you really do want to share your computer with another person regularly, make sure you know them well and trust them completely. Also, set up a separate account for them rather than give them any of your passwords.

If you believe your identity has been stolen, contact the Wisconsin Office of Privacy Protection at 1-800-422-7128 or email us at WisconsinPrivacy@datcp.state.wi.us. Visit our website at privacy.wi.gov for more information.